8011-01p

This document is scheduled to be published in the Federal Register on 11/04/2021 and available online at **federalregister.gov/d/2021-24035**, and on **govinfo.gov**

SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-93484; File No. 4-698]

Joint Industry Plan; Order Disapproving an Amendment to the National Market System Plan Governing the Consolidated Audit Trail

October 29, 2021.

I. Introduction

On December 18, 2020, the Operating Committee for Consolidated Audit Trail, LLC ("CAT LLC"), on behalf of the following parties to the National Market System Plan Governing the Consolidated Audit Trail (the "CAT NMS Plan" or "Plan"):[1] BOX Exchange LLC; Cboe BYX Exchange, Inc., Cboe BZX Exchange, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX Exchange, Inc., Cboe C2 Exchange, Inc., Cboe Exchange, Inc., Financial Industry Regulatory Authority, Inc. ("FINRA"), Investors Exchange LLC, Long-Term Stock Exchange, Inc., Miami International Securities Exchange LLC, MEMX, LLC, MIAX Emerald, LLC, MIAX PEARL, LLC, Nasdaq BX, Inc., Nasdaq GEMX, LLC, Nasdaq ISE, LLC, Nasdaq MRX, LLC, Nasdaq PHLX LLC, The NASDAQ Stock Market LLC, New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., NYSE Chicago, Inc., and NYSE National, Inc. (collectively, the "Participants," "self-regulatory organizations," or "SROs") filed with the Securities and Exchange Commission ("SEC" or "Commission") pursuant to Section 11A(a)(3) of the Securities Exchange Act of 1934 ("Exchange Act"),[2] and Rule 608 thereunder,[3] a proposed amendment ("Proposed Amendment" or "Proposal") to the CAT NMS Plan that would authorize

---

1 The CAT NMS Plan is a national market system plan approved by the Commission pursuant to Section 11A of the Exchange Act and the rules and regulations thereunder. See Securities Exchange Act Release No. 79318 (November 15, 2016), 81 FR 84696 (November 23, 2016) ("CAT NMS Plan Approval Order").

2 15 U.S.C 78k-1(a)(3).

3 17 CFR 242.608.

CAT LLC to revise the Consolidated Audit Trail Reporter Agreement (the "Reporter Agreement") and the Consolidated Audit Trail Reporting Agent Agreement (the "Reporting Agent Agreement" and collectively, the "Reporter Agreements") to insert limitation of liability provisions (the "Limitation of Liability Provisions").[4] The proposed plan amendment was published for comment in the Federal Register on January 6, 2021.[5]

On April 6, 2021, the Commission instituted proceedings pursuant to Rule 608(b)(2)(i) of Regulation NMS,[6] to determine whether to disapprove the Proposed Amendment or to approve the Proposed Amendment with any changes or subject to any conditions the Commission deems necessary or appropriate after considering public comment (the "OIP").[7] On June 25, 2021, the Commission designated a longer period within which to conclude proceedings regarding the Proposed Amendment.[8] On September 2, 2021, the Commission further designated a longer period within which to conclude proceedings regarding the Proposed Amendment.[9] This order disapproves the Proposed Amendment.

II. Background

On July 11, 2012, the Commission adopted Rule 613 of Regulation NMS, which required the SROs to submit a national market system ("NMS") plan to create, implement and maintain a

---

4 The Participants are requiring each CAT reporter or CAT reporting agent that reports order and trade data to the CAT System to execute a CAT Reporter Agreement or a CAT Reporting Agent Agreement. See, e.g., CAT FAQ O14, available at: https://www.catnmsplan.com/faq.

5 See Notice of Filing of Amendment to the National Market System Plan Governing the Consolidated Audit Trail, Release No. 90826 (December 30, 2020), 86 FR 591 (January 6, 2021) ("Notice").

6 17 CFR 242.608(b)(2)(i).

7 See Securities Exchange Act Release No. 91487 (April 6, 2021), 86 FR 19054 (April 12, 2021) ("OIP"). Comments received in response to the Notice and OIP can be found on the Commission's website at https://www.sec.gov/comments/4-698/4-698.htm.

8 See Securities Exchange Act Release No. 92266 (June 25, 2021), 86 FR 35142 (July 1, 2021).

9 See Securities Exchange Act Release No. 92854 (September 2, 2021), 86 FR 50201 (September 7, 2021).

consolidated audit trail (the "CAT" or "CAT System") that would capture customer and order event information for orders in NMS securities.[10] The Commission approved the CAT NMS Plan in 2016.[11]

On August 29, 2019, the Operating Committee for CAT LLC approved a Reporter Agreement that included a provision that would have limited the total liability of CAT LLC or any of its representatives to a CAT Reporter under the Reporter Agreement for any calendar year to the lesser of the total of fees paid by the CAT Reporter to CAT LLC for the calendar year in which the claim arose or five hundred dollars. The Participants required each Industry Member[12] to execute a CAT Reporter Agreement before reporting data to CAT. Prior to the commencement of initial equities reporting for Industry Members, the Securities Industry and Financial Markets Association ("SIFMA") filed on April 22, 2020, pursuant to Sections 19(d) and 19(f) of the Exchange Act, an application for review of actions taken by CAT LLC and the Participants (the "Administrative Proceedings"). SIFMA alleged that by requiring Industry Members to execute Reporter Agreements as a prerequisite to submitting data to the CAT, the Participants improperly prohibited or limited SIFMA members with respect to access to the CAT System in violation of the Exchange Act. On May 13, 2020, the Participants and SIFMA reached a settlement and terminated the Administrative Proceedings, allowing Industry Members to report data to the CAT pursuant to a Reporter Agreement that does not contain a limitation of liability provision. Since that time, Industry Members have been transmitting data to the CAT.[13]

III. Description of the Proposal

---

10 17 CFR 242.613.

11 See note 1, supra.

12 Industry Member means a member of a national securities exchange or a member of a national securities association. See CAT NMS Plan at Section 1.1.

13 For a more detailed description of the background for the Proposed Amendment, see Notice, supra note 5, at 591-93.

The Participants propose to amend the CAT NMS Plan to authorize CAT LLC to revise the Reporter Agreement and Reporting Agent Agreement with the proposed Limitation of Liability Provisions. As proposed, the Limitation of Liability Provisions would: (1) provide that CAT Reporters and CAT Reporting Agents accept sole responsibility for their access to and use of the CAT System, and that CAT LLC makes no representations or warranties regarding the CAT System or any other matter; (2) limit the liability of CAT LLC, the Participants, and their respective representatives to any individual CAT Reporter or CAT Reporting Agent to the lesser of the fees actually paid to CAT for the calendar year or $500; (3) provide that CAT LLC, the Participants, and their respective representatives shall not be liable for all direct and indirect damages of any kind or nature; and (4) provide that CAT LLC, the Participants, and their respective representatives shall not be liable for the loss or corruption of any data submitted by a CAT Reporter or CAT Reporting Agent to the CAT System.[14]

In support of the Proposed Amendment, the Participants state, among other things, that: (1) the proposed Limitation of Liability Provisions reflect longstanding principles of allocation of liability between Industry Members and SROs;[15] (2) the proposed Limitation of Liability Provisions "fall squarely within industry norms" and are consistent with exchange rules that limit liability for losses that members incur through their use of exchange facilities, provisions that FINRA members must agree to in order to comply with Order Audit Trail System ("OATS") reporting, and other provisions in the context of regulatory and NMS reporting facilities;[16] (3) previously granted exemptive relief that eliminated the requirement that CAT collect certain personally identifiable information, including social security numbers, makes the customer data stored in the CAT comparable to the data reported to other regulatory reporting facilities;[17] (4)

---

14 See Notice, supra note 5, at 593.

15 See Notice, supra note 5, at 593-95.

16 See Notice, supra note 5, at 593-94.

17 See Notice, supra note 5, at 595.

the proposed Limitation of Liability Provisions are necessary to ensure the financial stability of CAT because even though "CAT LLC has obtained the maximum extent of cyber-breach insurance coverage available and has implemented a full cybersecurity program to safeguard data stored in the CAT," there is "the potential for substantial losses that may result from certain categories of low probability cyberbreaches."[18]

CAT LLC retained Charles River Associates to conduct an economic analysis of the liability issues presented by a potential CAT breach (the "CRA Paper").[19] The Participants state that the analyses presented in the CRA Paper support the Participants' proposal to adopt a limitation of liability provision in the CAT Reporter Agreement and shows the importance of limiting CAT LLC's and each Participant's liability.[20] The CRA Paper asserts, among other things, that, based on an examination of potential breach scenarios and a consideration of the economic and public policy elements of various regulatory and litigation approaches to mitigate cyber risk for the CAT, a limitation of liability provision would serve the public interest by facilitating the regulation of the U.S. equity and option markets at lower overall costs and higher economic efficacy than other approaches, and that the proposed limitation on liability would not undermine CAT LLC's existing and significant incentives to protect the data stored in the CAT System. The CRA Paper asserts that regulation by the Commission already properly incentivizes the Participants to recognize and address the risks that a CAT cyber breach poses to third parties such as Industry Members. Thus, according to the Participants, permitting litigation by Industry Members will not meaningfully increase CAT's incentives to manage its exposure to cyber risk but will significantly increase costs, which will ultimately be passed on to retail investors. Because of this, the CRA Paper asserts that solely an "ex-ante regulation" approach leads to the socially optimal outcome, in comparison to an "ex post litigation" approach in which litigation

---

18 See Notice, supra note 5, at 595.

19 See Notice, supra note 5, at 599-624.

20 See Notice, supra note 5, at 595-597.

influences behaviors before a loss-producing event occurs by assigning liability afterwards, or combination of both approaches.

IV. Discussion

A. The Applicable Standard of Review

Under Rule 608(b)(2) of Regulation NMS, the Commission shall approve a national market system plan or proposed amendment to an effective national market system plan, with such changes or subject to such conditions as the Commission may deem necessary or appropriate, if it finds that such plan or amendment is necessary or appropriate in the public interest, for the protection of investors and the maintenance of fair and orderly markets, to remove impediments to, and perfect the mechanisms of, a national market system, or otherwise in furtherance of the purposes of the Exchange Act.[21] Under Rule 700(b)(3) of the Commission's Rules of Practice, the "burden to demonstrate that a proposed rule change is consistent with the Exchange Act and the rules and regulations issued thereunder . . . is on the self-regulatory organization that proposed the rule change."[22] The Commission shall disapprove a national market system plan or proposed amendment if it does not make such a finding.[23]

For the reasons described below, the Commission believes that the Participants have not met their burden to demonstrate that the Proposed Amendment is consistent with the Exchange

---

21 17 CFR 242.608(b)(2).

22 17 CFR 201.700(b)(3).

23 17 CFR 242.608(b)(2). Approval or disapproval of a national market system plan, or an amendment to an effective national market system plan (other than an amendment initiated by the Commission), shall be by order. Id. In addition, Rule 700(b)(3)(ii) of the Commission's Rules of Practice states that "[t]he burden to demonstrate that a NMS plan filing is consistent with the Exchange Act and the rules and regulations issued thereunder that are applicable to NMS plans is on the plan participants that filed the NMS plan filing." 17 CFR 201.700(b)(3)(ii). "Any failure of the plan participants that filed the NMS plan filing to provide such detail and specificity may result in the Commission not having a sufficient basis to make an affirmative finding that a NMS plan filing is consistent with the Exchange Act and the rules and regulations issued thereunder that are applicable to NMS plans." Id.

Act.[24] Accordingly, the Commission cannot make the finding that the Proposed Amendment is necessary or appropriate in the public interest, for the protection of investors and the maintenance of fair and orderly markets, to remove impediments to, and perfect the mechanisms of, a national market system, or otherwise in furtherance of the purposes of the Exchange Act.[25]

B. Impact of Proposed Amendment on Incentives of Participants
Incentives to Invest in Security of the CAT

The Commission received several comments, including a letter from SIFMA attaching an economic analysis prepared by Craig Lewis ("Lewis Paper") of the Proposed Amendment,[26] expressing concern that shifting liability through a limitation of liability provision would reduce the incentives of Participants to develop robust data security and risk mitigation mechanisms, and may even incentivize the Participants to de-prioritize data security.[27] Commenters also state

---

24 17 CFR 201.700(b)(3).

25 17 CFR 242.608(b)(2).

26 See Letter from Ellen Greene, Managing Director, Equity and Options Market Structure, SIFMA, to Vanessa Countryman, Secretary, dated February 19, 2021, available at https://www.sec.gov/comments/4-698/4698-8394069-229410.pdf, attaching Economic Analysis of Proposed Amendment to National Market System Plan Governing the Consolidated Audit Trail, Craig M. Lewis, Ph.D., February 2021.

27 See Lewis Paper at 5-9, 14; Letter from Ellen Greene, Managing Director, Equity and Options Market Structure, SIFMA, to Vanessa Countryman, Secretary, dated January 27, 2021, available at https://www.sec.gov/comments/4-698/4698-8298026-228278.pdf ("SIFMA Letter"), at 7, 9; Letter from Peggy L. Ho, Executive Vice President, Government Relations, LPL Financial LLC, to Vanessa Countryman, Secretary, dated January 27, 2021, available at https://www.sec.gov/comments/4-698/4698-8298412-228298.pdf ("LPL Financial Letter"), at 1; Letter from Thomas R. Tremaine, Executive Vice President, Chief Operations Officer, Raymond James & Associates, Inc., to Vanessa Countryman, Secretary, dated February 8, 2021, available at https://www.sec.gov/comments/4-698/4698-8347733-229000.pdf ("Raymond James Letter"), at 2; Letter from Joanna Mallers, Secretary, FIA Principal Traders Group, to Vanessa Countryman, Secretary, dated February 8, 2021, available at https://www.sec.gov/comments/4-698/4698-8345389-228979.pdf ("FIA PTG Letter"), at 2; Letter from Thomas M. Merritt, Deputy General Counsel, Virtu Financial, Inc., to Vanessa Countryman, Secretary, dated January 27, 2021, available at https://www.sec.gov/comments/4-698/4698-8298023-228258.pdf ("Virtu Letter"), at 3; Letter from Christopher A. Iacovella, Chief Executive Officer, American Securities Association, to Vanessa Countryman, Secretary, dated January 29, 2021, available at https://www.sec.gov/comments/4-698/4698-8311307-228499.pdf ("ASA Letter"), at 2; Letter from Matthew Price, Fidelity Investments, to Vanessa Countryman, Secretary,

that it is "unfair" for Industry Members to be liable for breaches of the CAT or CAT Data[28] because the Participants, through CAT LLC, and FINRA CAT, the Plan Processor,[29] are the parties responsible for controlling and securing CAT Data and Industry Members face potential harm due to the compromise of CAT Data over which they have no control and are not responsible for security.[30] The Lewis Paper argues that aligning control and liability incentivizes the optimal amount of data security and would ultimately benefit all investors.[31] Along the same lines, another commenter asserts that "[a]ligning control and liability is not only fair and equitable; it is also good policy, because it maximizes efficiencies in managing data risks inherent in the CAT System."[32]

---

dated February 2, 2021, available at https://www.sec.gov/comments/4-698/4698-8343750-228940.pdf ("Fidelity Letter"), at 2; Letter from Daniel Keegan, Managing Director, Head of North America Markets & Securities Services, to Vanessa Countryman, Secretary, dated February 25, 2021, available at https://www.sec.gov/comments/4-698/4698-8419819-229522.pdf ("Citi Letter"), at 2.

28 "CAT Data" means data derived from Participant Data, Industry Member Data, SIP Data, and such other data as the Operating Committee may designate as "CAT Data" from time to time. See CAT NMS Plan at Section 1.1.

29 "Plan Processor" means the Initial Plan Processor or any other Person selected by the Operating Committee pursuant to SEC Rule 613 and CAT NMS Plan, Article IV, Section 4.3(b)(i) and Article VI, Section 6.1, and with regard to the Initial Plan Processor, the Selection Plan, to perform the CAT processing functions required by SEC Rule 613 and set forth in this Agreement. See CAT NMS Plan at Section 1.1.

30 See Lewis Paper at 3, 6; SIFMA Letter, at 4; FIA PTG Letter, at 1 (stating it "supports the comments previously filed by SIFMA"); Raymond James Letter, at 2 (stating that it "strongly supports the points raised by SIFMA in their letter."); LPL Financial Letter, at 1; ASA Letter, at 2; Virtu Letter, at 2; Fidelity Letter, at 2; Citi Letter, at 2; Letter from Ellen Greene, Managing Director, Equity and Options Market Structure, SIFMA, to Vanessa Countryman, Secretary, dated May 3, 2021 ("SIFMA Letter II") at 2; 4; Letter from Kelvin To, Founder and President, Data Boiler Technologies, LLC, to Vanessa Countryman, Secretary, dated May 3, 2021 ("Data Boiler Letter II") at 5.

31 See Lewis Paper at 5-7; see also SIFMA Letter II at 2-3, 9-10.

32 See SIFMA Letter at 4. One commenter states that the CAT System is a particularly attractive target for nation states and other bad actors that have become increasingly sophisticated, which could lead to significant harm to market participants, serious competitive harm to Industry Members, and significant legal risk and potential liability. See SIFMA Letter II at 9.

Commenters argue that the CRA Paper's specific conclusion that ex-ante regulation is most appropriate is wrong, and that CAT cybersecurity would benefit from both ex-ante regulation and ex-post litigation.[33] Another commenter characterizes shifting liability to Industry Members who, unlike SROs, have no control over the security of the CAT as creating a "moral hazard" and stated that permitting litigation against Participants and their representatives when they are acting outside their regulatory capacity is "crucial" as it would give the Participants very strong financial incentives to invest heavily to prevent or minimize the likelihood of such failures.[34] Similarly, the Lewis Paper asserts that liability for potential litigation would mitigate the moral hazard problem for CAT LLC and make CAT LLC more willing to invest in improvements in data security and more quickly react to changing trends and threats in cybersecurity.[35]

In response to the Lewis Paper's contention that the threat of ex-post litigation is necessary, the CRA Response asserts that the "inconsequential and speculative" benefits of litigation in addition to the existing regulatory regime do not exceed the likely substantial costs.[36]

---

33 See Letter from Stephen John Berger, Managing Director, Global Head of Government & Regulatory Policy, Citadel Securities, to Vanessa Countryman, Secretary, dated February 23, 2021, available at https://www.sec.gov/comments/4-698/4698-8411798-229501.pdf ("Citadel Letter"), at 1-2, 7; Lewis Paper at 7-9. SIFMA states that the Lewis Paper, submitted by SIFMA, concludes that the Proposal would reduce investor welfare by: (1) providing less incentive to the SROs as the operators of the CAT to invest in data security to protect investors' personally identifiable information and trading data in the CAT, which would place investors at greater risk of having their data compromised; and (2) leading to the inefficient purchase of insurance with additional costs likely passed downstream to investors by requiring industry members to absorb litigation-related expenses for an event over which they have no direct control. See SIFMA Letter II at 3.

34 See Citi Letter at 2, 7, 9-10.

35 See Lewis Paper at 7-9.

36 See Report from Charles River Associates, "CRA Response to: Economic Analysis of Proposed Amendment to the National Market System Plan Governing the Consolidated Audit Trail by Craig M. Lewis, Ph.D. and Selected Points in Public Comment Letters," dated April 5, 2021, available at https://www.sec.gov/comments/4-698/4698-8634778-230925.pdf ("CRA Response") at 9. The CRA Response further states that the Lewis Paper mischaracterized this argument as meaning that the CRA Paper said there are no benefits to adding the threat of litigation. Id.

The CRA Response further asserts that there is no asset reserve on the balance sheet of CAT LLC sufficient to cover a substantial cyber loss, and thus, adding a threat of litigation may not provide any additional incentives to invest in preventative care.[37]

The Participants argue that securities industry norms do not support the principle that the party in possession of data should bear liability in the event of a data breach, particularly where the parties in possession of the data are acting in regulatory capacities pursuant to Commission rules.[38] In this regard, the Participants state that Industry Members, despite controlling sensitive data that could be compromised during a data breach, "routinely" disclaim liability to their underlying customers including their own retail customers in certain cases.[39]

The Participants also assert that the Commission's regulatory regime, backed by its examination and enforcement functions, provide valuable incentives for the Participants, CAT LLC and FINRA CAT to take adequate cyber security precautions.[40] These incentives include the Commission's enforcement regime, severe reputational harm, financial and reputational harm to Amazon Web Services, satisfying underwriting standards, and the fact that a data breach could compromise the Participants' ability to use CAT Data.[41] The Participants believe that commenters have not offered any explanation as to why the Commission's regulatory regime—

---

37 See CRA Response at 4. See also CRA Response at 9 (stating that CAT LLC's "cost-only business model" provides no mechanism to establish safety reserves that might allow it to build a cash reserve to pre-fund catastrophic losses from a cyber breach).

38 See Letter from Michael Simon, CAT NMS Plan Operating Committee Chair, to Vanessa Countryman, Secretary, dated April 1, 2021 ("Response Letter"), at 10.

39 See Response Letter at 10; see also id. at 20 (stating that the Lewis Paper does not address the fact that Industry Members routinely disclaim liability to those underlying customers).

40 See, e.g., Letter from Michael Simon, CAT NMS Plan Operating Committee Chair, to Vanessa Countryman, Secretary, dated May 18, 2021, available at https://www.sec.gov/comments/4-698/4698-8811359-238002.pdf ("Second Response Letter"), at 3, 5-7. The Participants state that CAT LLC, the Participants and FINRA CAT are subject to stringent oversight by the Commission. In addition, the Division of Examinations examines FINRA CAT's and the Participant's cybersecurity policies, procedures, systems, and controls. See Second Response Letter at 6-7 (also citing Second Circuit decision in support).

41 See Second Response Letter at 5-6. See also CRA Response at 1, 3-4, 6-7, 10.

which includes cybersecurity protocols developed and refined based on feedback from Industry Members—is insufficient to ensure adequate cybersecurity for CAT Data, or what deficiencies in the Commission's oversight necessitate that Industry Members be afforded an unprecedented private right of action against their regulators.[42] The Participants further argue that commenters have not demonstrated that the Commission lacks the ability to adequately regulate the CAT and the Participants, and that allowing Industry Member litigation would not result in any meaningful benefit to the CAT's cybersecurity.[43] In addition, the CRA Response states that the Lewis Paper disregards the potential for enforcement action by the Commission against Participants and does not recognize that regulatory and reputational considerations motivate appropriate ex-ante actions to reduce risk.[44]

Commenters also state that the CRA Paper suggests certain mechanisms, such as a third-party compensation program, cyber-related industry loss warranties or cyber catastrophe bonds that could be used in the event of a CAT breach to compensate third parties, but the SROs have not proposed the adoption of any of these mechanisms.[45] These commenters believe that without liability risk, CAT LLC and the SROs will have no incentive to develop any mechanisms for

---

42 See Response Letter at 26.

43 See Second Response Letter at 3.

44 See CRA Response at 5-6. The CRA Response states that there are several weaknesses with the Lewis Paper's and the Citadel Letter's argument that litigation as well as regulation is necessary to give CAT LLC an added incentive to stay ahead of the Commission's regulation since the underlying technology changes come too fast for the Commission to keep its regulatory apparatus up to date: (1) Lewis and Citadel ignore that Participants and FINRA CAT are required to monitor CAT's cyber security and promptly address vulnerabilities in accordance with Commission regulation; (2) Industry Members can influence CAT LLC and Commission regarding cybersecurity as a result of CAT LLC governance and operating mechanisms; (3) Commission has unique access to highly sophisticated cyber security and cyber warfare assets, which give them access to the most up-to-date technology; (4) CAT's technology suppliers (e.g., AWS) have reputational incentives to maintain CAT cyber defenses; (5) the ability to litigate might increase CAT cyber risk by potentially weakening Industry Members' incentives to provide feedback to the Participants; (6) Participants still face litigation risk including from Commission enforcement actions. See CRA Response at 13-14.

45 See SIFMA Letter at 10; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2.

compensating third parties injured if the CAT System is breached or CAT Data is misused while under the control of CAT LLC and the SROs.[46] These commenters assert that the Participants, are effectively conceding that without these other mechanisms described in the CRA Paper, the current regulatory regime is insufficient to protect parties that are injured as a result of a CAT breach.[47]

The Participants acknowledge that the CRA Paper explains that the regulatory regime is generally silent with respect to the most efficient method to compensate injured parties and that the CRA Paper offered several suggestions to cover potential losses including insurance, industry loss warranties, and catastrophe bonds.[48] The Participants, however, state that they are willing discuss any of these compensation mechanisms with Industry Members and they would welcome a discussion with the Commission to address the viability of these mechanisms and how they might be funded.[49]

Cyber Insurance

Commenters assert that the proposal would allow CAT LLC to under-invest in data security and cyber insurance.[50] Commenters argue that the Proposed Limitation of Liability Provisions would ultimately result in higher costs borne by investors.[51] According to commenters, under the proposal, every firm submitting data to the CAT System would effectively be forced, where possible, to obtain its own insurance to address the same core risks of data breach or misuse within the CAT System and CAT LLC and the Participants may not be

---

46 See id.

47 See id.

48 See Response Letter at 27 (citing CRA Paper at 50-53).

49 See Response Letter at 27-28. The Participants also state that creating mechanisms to compensate Industry Members in the event of a data breach would not obviate the need for the proposed Limitation of Liability Provisions. See id. at 28.

50 See SIFMA Letter II at 2-3, 9-10; Lewis Paper.

51 See SIFMA Letter II at 2-3, 9-10; Lewis Paper.

appropriately incentivized to invest in insurance and other risk mitigation mechanisms.[52] Commenters believe that it would be more appropriate for CAT LLC to purchase insurance instead of Industry Members each purchasing the same overlapping policies.[53] One of these commenters argues that CAT LLC is able to insure more efficiently than Industry Members because CAT LLC has access to and control over CAT Data and systems and can subject itself to monitoring by an insurer.[54] One commenter states that while the Participants assert that CAT LLC has obtained the "maximum extent of cyber-breach insurance coverage," the Participants have not disclosed any information about the extent or cost of the coverage obtained,[55] and do not analyze whether Participants should seek insurance or the effect such insurance could have on the Participants' incentives to protect data that they extract from the CAT and store outside the CAT.[56] The commenter states that it is not at all clear that CAT LLC could not obtain additional insurance.[57]

The Participants reiterate that CAT LLC has purchased the maximum amount of cyber insurance coverage that the current market will reasonably provide. The Participants also state that they will regularly evaluate CAT LLC's insurance and intend to purchase additional

---

52 See SIFMA Letter II at 10. See also Data Boiler Letter II at 3 (provisions discourage Participants from advancing the security and design of CAT and CAT Data).

53 See Lewis Paper at 11; SIFMA Letter at 4-5, 8-9, 10-11; Virtu Letter at 3. See also LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2. One commenter expresses skepticism that Industry Members could even obtain insurance policies under the current CAT System construct, because Industry Members have no control over the data they are by law required to submit, its security or the CAT System. See Virtu Letter at 3.

54 See Lewis Paper at 12-13. See also SIFMA Letter at 4-5 (stating that requiring Industry Members to pay for and implement separate and overlapping insurance policies, if available, is inefficient and would result in substantially higher costs borne by Industry Members and by extension their customers).

55 See SIFMA Letter II at 9.

56 See Citadel Letter at 7-8. See also Lewis Paper at 13-14.

57 See SIFMA Letter II at 9. SIFMA also discusses the state of negotiations with the Participants. See SIFMA Letter II at 11.

coverage to the extent it becomes reasonably available.[58] The Participants argue that disclosing the amount of insurance purchased by CAT LLC could potentially incentivize bad actors to target the CAT with ransom demands.[59] The Participants assert that CAT LLC is not equipped to compensate Industry Members in the event of a data breach because funding is designed to cover costs only and it is difficult to imagine how CAT LLC could ensure solvency if substantial exclusions are included in a limitation of liability.[60] The CRA Response states that the Lewis Paper's conclusion that the Participants should purchase additional cyber-insurance relies on two propositions for which the Lewis Paper provides no basis: (1) CAT LLC can purchase additional and more targeted cyber insurance to pre-finance possible cyber claims from Industry Members and that (2) the decrease in cyber security risks and insurance rates to Industry Members would outweigh the increase in CAT LLC's cyber insurance rates.[61]

The CRA Response asserts that the Lewis Paper's claim that the Limitation of Liability Provisions will force clients' claims onto Industry Members and burden Industry Members with purchasing additional insurance coverage is erroneous.[62] Specifically, according to the CRA Response, the Lewis Paper does not explain how Industry Members' clients can sue Industry Members for a cyberbreach of CAT, does not consider that many Industry Members have similar provisions in their customer agreements, and does not explain how an insurer would write liability coverage for Industry Members paying claims to clients for an adverse cyber event.[63] In

---

58 See Second Response Letter at 17.

59 See Second Response Letter at 17. The Participants noted that they were reviewing a May 3, 2021 term sheet from SIFMA setting forth terms upon which Industry Members would be willing to resolve the dispute regarding the allocation of liability in the event of a CAT data breach. Id.

60 See Second Response Letter at 15.

61 See CRA Response at 5.

62 See CRA Response at 5-6.

63 See CRA Response at 5-6. However, purchasing cyber liability insurance to protect against potential first-party risk exposure might be part of a reasonable and sound approach to managing first-party risk exposure. Id. at 13.

addition, the CRA Response states that the Lewis Paper and commenters assume, without support, that Industry Members will face litigation risk from customers due to a cyberbreach at the CAT.[64]

Visibility and Input of Industry Members Into the Security of the CAT

One commenter argues that the CRA Paper significantly overemphasizes the visibility and input into the workings of CAT provided to the industry, and asserts that there is no visibility into the security aspects of CAT.[65] The Participants state that Industry Members have had extensive opportunities to provide input regarding the CAT's cybersecurity at every stage of the development and operation of the CAT.[66] The CRA Response states that commenters fail to acknowledge that providing Industry Members a right to litigate may reduce Industry Members' incentives to undertake their monitoring and influencing activities in favor of relying upon the threat of litigation, thereby weakening the overall cyber program of the CAT.[67] The CRA Response also states that limiting Industry Members' ability to recover damages provides greater incentives for them to provide feedback to CAT management through the Advisory Committee.[68]

Regulatory Immunity

Commenters argue that the SROs have failed to explain why limitation of their liability should be imposed by contract because the SROs have immunity from liability when acting in a regulatory capacity.[69] Commenters further assert that the effort to impose liability limitations by

---

64 See CRA Response at 13.

65 See Citadel Letter at 9.

66 See Response Letter at 14. This includes prior to approval of the CAT NMS Plan, feedback through the Advisory Committee, and the ability of Industry Members to directly petition the Commission or provide comments on any proposals offered by the Commission. Id.

67 See CRA Response at 2, 9, and 11.

68 See CRA Response at 19. The Participants also assert that Industry Members have ample opportunities to contribute their perspectives regarding the CAT's cybersecurity. See Second Response Letter at 10.

69 See Citadel Letter at 1, 3-5; SIFMA Letter at 8; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2; SIFMA Letter II at 5; 6-7.

contract "raises significant questions about whether the SROs seek to avoid liability in circumstances in which they misuse CAT Data while acting in a commercial capacity."[70] Another commenter frames the issue as not whether the Participants should be liable for conduct undertaken during the course of their regulatory responsibilities, but whether the Participants should be insulated from potential liability for activities not covered by regulatory immunity.[71] One commenter states that it believes that court precedent "strongly indicates that the courts are likely to view any regulatory activity the SROs conduct through CAT LLCs as being subject to this judicial immunity even though it is being conducted in a legal entity that is separate from the SROs."[72]

In response to comments about regulatory immunity, the Participants state that regulatory immunity does not preclude the use of contractual limitation of liability provisions and the divergent and shifting positions from Industry Members on the applicability of regulatory immunity underscores the need for a contractual limitation of liability.[73] The Participants state that some comments generally argue that a contractual limitation of liability is unnecessary in light of the doctrine of regulatory immunity, while other comments state the Participants should not receive either regulatory immunity or the protection of a limitation of liability provision.[74] The Participants state that the proposed Limitation of Liability Provisions are necessary despite any regulatory immunity because even litigation which holds that regulatory immunity applies may result in significant disruption and expense (which ultimately will be passed along to

---

70 See SIFMA Letter at 8. See also LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2.

71 See Citadel Letter at 5.

72 See SIFMA Letter II at 7. See also Data Boiler Letter II at 4.

73 See Response Letter at 22-25; see also Second Response Letter at 4, 11-12. The Participants also state that SIFMA has not indicated that it and constituent Industry Members will abandon their extensive efforts to challenge the regulatory immunity doctrine in court or cease lobbying Congress to abrogate it by statute. Id. at 3-4, 11.

74 See Response Letter at 21-23. The Participants state that SIFMA's longstanding position is that Congress should abrogate regulatory immunity by statute. Id. at 23-24.

Industry Members as part of CAT LLC's joint funding), and there is no guarantee that all courts would agree that the Participants' immunity defense extends to the particular claims at issue.[75] The Participants believe that the Proposed Limitation of Liability Provisions are necessary to avoid the uncertainty inherent in litigation and to avoid the costs associated with defending against potential lawsuits.[76] In addition, litigation would be costly and resource intensive and ultimately distract the Participants and FINRA CAT from their important regulatory oversight mandate.[77] The Participants state that several commenters misstate the scope of the Proposed Amendment by suggesting that the Proposed Amendment would extinguish liability.[78] The Participants state that the Proposed Amendment only concerns the allocation of liability between Industry Members and the Participants and the Proposed Amendment would not impact the rights or obligations of third parties, including Industry Members' customers and would not extinguish the broad regulatory oversight that the Commission exercises over the CAT or potential investigation and potential enforcement action for any cybersecurity-related violations.[79]

The Participants believe that commenter concerns that the regulatory process might not keep pace with emerging and evolving cyber threats fails to consider Commission regulatory requirements and oversight, including the CAT NMS Plan requirement that Participants and FINRA CAT proactively monitor the CAT's cybersecurity and promptly address any vulnerabilities.[80] Participants state, in contrast, litigation would require the Commission to share responsibility with the courts and is a lengthy process that is unlikely to outpace regulation.[81] In

---

75 See Response Letter at 23-25. See also Second Response Letter at 4, 11.

76 See Second Response Letter at 11-12.

77 See id.

78 See Response Letter at 25 (citing Citi Letter at 2 and SIFMA Letter at 9).

79 See Response Letter at 25-26.

80 See Second Response Letter at 7.

81 See Second Response Letter at 8.

addition, the Commission has means other than the formal rule-making process to address emerging cyber threats.[82] In addition, the Participants assert that allowing Industry Member litigation would undoubtedly result in substantial additional costs and that the CRA Paper demonstrates that the costs of litigating a potential CAT Data breach are likely to be both substantial and unquantifiable on an ex-ante basis.[83] It would also create additional costs and distract the Participants from the regulatory mission of CAT, and these costs would ultimately be passed along to investors.[84] The Participants state that commenters are asking that their primary regulators bear any and all liability for hypothetical "black swan" cyber breaches and that such an extraordinary ask is without precedent, and that Participants, implementing a regulatory mandate in their regulatory capacities, should receive liability protections that they are customarily afforded when implementing their regulatory responsibilities pursuant to the direction and oversight of the Commission.[85]

CRA Paper Does Not Capture All Data Breach Risks and Costs

Commenters believe that the CRA Paper does not capture all data breach risks, stating that the CRA Paper only focuses on a breach by external actors and fails to address the risk of

---

82 See Second Response Letter at 8. The Participants state that the Commission and its staff have "multiple tools at their disposal to motivate regulated entities" to "expeditiously modify their cybersecurity regimes." "For example, the Division of Examinations, which has prioritized cybersecurity issues, often releases risk alerts in response to emerging concerns." Id.

83 See Second Response Letter at 3-4, 16.

84 See Second Response Letter at 4, 16.

85 See Second Response Letter at 4; see also Response Letter at 20 (stating that the Lewis Paper appears to advocate that CAT LLC should be strictly liable for all costs associated with any CAT data breach, regardless of the facts and circumstances, without any economic analysis as to why the longstanding allocation of liability between the Participants and Industry Members should not apply here). The Participants note that both the Participants and Industry Members are acting pursuant to Commission mandate, but the Participants are also fulfilling a regulatory oversight role and there is no basis for the Participants to assume liability. See Response Letter at 21. See also Second Response Letter at 4.

misuse of CAT Data by personnel at CAT LLC and the SROs.[86] In addition, one commenter emphasizes that the CRA Paper focuses on databases maintained by CAT LLC, not the "larger concern," which is the potential for hackers to access CAT Data from Participant databases that have extracted data from the CAT.[87] Two commenters further criticize the breach scenarios discussed in the CRA Paper as insufficient to capture the risks. One of these commenters suggests that a breach of CAT by foreign actors, or CAT being internally compromised could lead to the "downfall" of U.S. capital markets and that the breach scenarios in the CRA Paper "grossly" underestimate national security threats.[88] Another commenter states that the CRA Paper "avoids any serious discussion" of the risk posed by "nation state actors, like China and Russia."[89]

Participants and the CRA Response dispute commenters' claims that the CRA Paper does not include all potential data breaches.[90] The Participants argue that certain commenters misconstrue the CRA Paper's analysis.[91] Specifically, these commenters assert that the CRA Paper did not address certain categories of hypothetical data breaches, and in particular breaches that originate from within FINRA CAT or Participants. The Participants state that the CRA

---

86 See Citadel Letter at 6; SIFMA Letter at 9; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2; Virtu Letter at 5. One commenter states that the CRA Paper does not provide any support for the argument that broker-dealers should be accountable for the wrongdoing or misuse of data by SRO employees or contractors. See ASA Letter at 2.

87 See Citadel Letter, at 6-7.

88 See Letter from Kelvin To, Founder and President, Data Boiler Technologies, LLC, to Vanessa Countryman, Secretary, dated January 27, 2021, at 1 and 6, available at https://www.sec.gov/comments/4-698/4698-8311309-228460.pdf.

89 See ASA Letter at 2.

90 See Response Letter at 15. The Participants explain that the CRA Paper contain two principal analyses: (i) a "scenario analysis" in which it identified specific hypothetical breaches and assessed the relative difficulty of implementation, relative frequency, and conditional severity of each; and (ii) a consideration whether the cyber risk presented by the CAT should be addressed by regulation, litigation, or a combination of both approaches.

91 See Response Letter at 15.

Paper did not make any assumptions regarding the identity of potential bad actors or where they may work, and the CRA Paper was not intended to predict every possible scenario, but instead intended to provide an illustrative framework to assess the economic exposures that flow from the gathering, storage, and use of CAT Data.[92] The Participants state that the CRA Paper concludes, in light of the CAT's extensive cybersecurity and other reasons, most potential breaches are relatively low-frequency events because they are either difficult to implement, unlikely to be meaningfully profitable, or both.[93] The Participants also believe that the CRA Paper's conclusion that allowing Industry Members to litigate against CAT LLC, the Participants, and FINRA CAT would provide minimal benefits while imposing substantial costs is not undermined to the extent that commenters identify potential breaches that were not included in the CRA Paper's scenario analysis.[94]

The Participants believe that comments that criticize the CRA Paper for failing to consider the costs to individual Industry Members in the event of a CAT Data breach are based on a misunderstanding of the relevant economic principles.[95] Specifically, the CRA Paper's focus was on whether the risks of the use of CAT Data for regulatory purposes was best managed through ex ante regulation or ex post litigation, or a combination of both, and this analysis largely turns on identifying the most effective and efficient mechanisms for incentivizing CAT LLC, the Participants and FINRA CAT to take appropriate precautions.[96] The Participants state that the CRA Paper demonstrates that the extensive regulatory regime that the Commission has enacted creates appropriate and strong incentives for the Participants to take sufficient cybersecurity precautions and to ensure that the CAT is secure, and that allowing

---

92 See Response Letter at 15-16 (citing CRA Paper 2).

93 See Response Letter at 16 (citing CRA Paper at 18-32).

94 See Response Letter at 16.

95 See Response Letter at 16.

96 See id.

Industry Members to litigate against Participants would create substantial costs without any corresponding benefit.[97]

The CRA Response states that allowing Industry Members to litigate against CAT LLC and Participants entails potentially substantial costs and uncertainty in the operation of the CAT that, ultimately, could be borne by Industry Members' underlying customers,[98] as a result of the Commission-approved joint funding of CAT LLC by Industry Members and Participants, a fact the CRA Response believes that the Lewis Paper ignores. According to the CRA Response, a limitation of liability also protects Industry Members from the possibility of funding both catastrophic losses and substantial litigation costs.[99]

Participants and the CRA Response argue that the Lewis Paper's argument that CAT LLC is in a better position to insure against a CAT Data breach fails because, among other reasons, it is based on a premise that a cyberbreach would impact all Industry Members simultaneously[100] and ignores the fact that CAT LLC has already purchased the maximum insurance coverage that was feasibly available.[101] The CRA Response states that the CRA Paper's scenario analysis does not support the Lewis Paper's assertion that a breach is likely to be a single event that affects all Industry Members simultaneously, and the Lewis Paper does not explain why a single event instead of multiple events affecting subsets of Industry Members might make a difference.[102] The Commission acknowledges that a number of factors impact the

---

97 See Response Letter at 16-17. The Participants also dispute an assertion that the CRA Paper delivered a "pre-determined conclusion." See id. at 17 (citing ASA Letter at 2-3).

98 See CRA Response at 8.

99 See CRA Response at 2, 8.

100 The Participants state that the Lewis Paper does not include a scenario analysis like the CRA Paper. See Response Letter at 16 at 20-21.

101 See CRA Response at 2, 4-5.

102 See CRA Response at 16. The CRA Response also states that the Lewis Paper also implies that a single event is unlike a typical situation where pooling of risk can reduce the volatility around claims, but the CRA Response further argues this is a narrow view as insurers can spread correlated risks through reinsurance contracts across the global insurance industry ultimately bringing the benefits of diversification to all who are

Participants' incentives to invest in, or prioritize, the security of the CAT. These factors include, but are not limited to (in no specific order): the cost of security; regulatory requirements, including Commission supervision and enforcement, fines, penalties and potential loss of their SRO licenses; reputation; the threat of litigation; and the amount of potential payments to those impacted by a security breach. Given the sensitivity of CAT Data, as well as the importance of the CAT for regulatory purposes, the Commission believes it is important to evaluate the incentives to invest in, or prioritize, the security of the CAT. The burden is on Participants to demonstrate that the Proposed Amendment is necessary or appropriate in the public interest, for the protection of investors and the maintenance of fair and orderly markets, to remove impediments to, and perfect the mechanisms of, a national market system, or otherwise in furtherance of the purposes of the Exchange Act.[103] Accordingly, the Commission believes that the Participants must demonstrate that the Proposed Amendment satisfies this standard in light of its potential impact on the Participants' incentives to invest in or prioritize the security of CAT.

By essentially eliminating any potential liability to Industry Members in the event of a security breach, the Participants limit the risk to themselves should they decide to reduce their investments in the security of the CAT, and such a reduction could increase the potential for a breach of CAT or unauthorized release of CAT Data. The Participants characterize one of the potential liabilities that they need to be insulated from as "the potential for substantial losses that may result from certain categories of low probability cyberbreaches,"[104] and the CRA Paper estimates an exposure of at least $100 million per incident as a "reasonable" estimate for a data breach scenario in which an algorithmic trading firm's strategy was reverse engineered, which it also describes as very difficult to implement and occurring infrequently.[105] The Proposed

---

insured. Id.

103 17 CFR 201.700(b)(3).

104 See Notice, supra note 5, at 595.

105 See Notice, supra note 5, at 597, 599-600, 603.

Amendment would almost completely insulate the Participants from any liability to member firms for those damages. Due to potentially lower costs should such a breach occur, the Commission believes the proposed Limitation of Liability Provisions would have a negative impact on the incentives of Participants to secure the CAT to prevent breaches, including purportedly low probability events.[106] Also, absent the proposed Limitation of Liability Provisions, the Participants might be incentivized to make further investments in data security beyond those mandated by the CAT NMS Plan and Commission rulemakings, such as internal controls designed to decrease the likelihood of misuse of CAT Data beyond the requirements of the CAT NMS Plan.

The CRA Response states that the benefits of litigation in addition to the existing regulatory regime are "inconsequential and speculative" and do not exceed the likely substantial costs.[107] However, the CRA Response acknowledges that the threat of liability does incentivize behavior, arguing that limiting Industry Members' ability to recover damages provides greater incentives for them to provide feedback to CAT management through the Advisory Committee.[108] The Commission believes that although Industry Members do have avenues to provide feedback such as through the Advisory Committee, Industry Members do not have access to the information they would need, such as security audit results and design specifications, to evaluate the security of CAT and identify meaningful deficiencies. The Commission also believes that the CRA Response's argument applies to Participants, in that their behavior would change to the extent there is a decreased threat of liability. Specifically, with the proposed Limitation of Liability Provisions, the Participants' potential liability to Industry

---

106 See also Economic Analysis at Section V.A.

107 See CRA Response at 9. Neither the Participants nor the CRA Paper or CRA Response provides specifics regarding estimated costs of litigation.

108 See CRA Response at 19.

Members would decrease and thus reduce Participants' incentives to ensure robust cybersecurity of CAT and CAT Data in an effort to reduce or avoid the potential liability.

Participants argue that security industry norms do not support the principle that the party in possession of the data should bear liability in the event of a data breach, especially when acting in a regulatory capacity pursuant to Commission rules,[109] and that Industry Members "routinely" disclaim liability to their underlying customers.[110] The Commission did not approve provisions in Industry Member contracts for OATS or Industry Member contracts with underlying customers. The Participants also refer to limitation of liability provisions in SROs' rules that were previously approved by the Commission.[111] In the case of the SROs' rules, these rules relate to liability to members with respect to the business operations of exchanges and were established for different types of systems with different risks than the CAT.[112] The Commission believes that given the amount and sensitivity of the data in the CAT System, it is important that the Participants' incentives to invest in robust cybersecurity, including potential liability in the event of a breach, are not reduced. Based on the record before it, the Commission believes that the proposed Limitation of Liability Provisions would reduce Participants' incentives to invest in CAT Data security.

The CRA Response also states that providing Industry Members a right to litigate may reduce Industry Members' incentives to undertake their monitoring and influencing activities in favor of relying upon the threat of litigation, thereby weakening the overall cyber program of the CAT.[113] The Commission also believes that these comments suggest that Industry Members can

---

109 See Response Letter at 10.

110 See Response Letter at 10; see also Response Letter at 20 (stating that the Lewis Paper does not address the fact that Industry Members routinely disclaim liability to those underlying customers).

111 See Response Letter at 5-7.

112 CAT Data, unlike an SRO's trading data, includes comprehensive trading data from all exchange SROs and order and customer information submitted by Industry Members.

113 See CRA Response at 2, 9, and 11.

have a significant role in determining the strength of the overall cyber program of CAT, and if a reduction in Industry Member "monitoring and influencing activities" would weaken the overall cyber program of the CAT, the absence of essentially any liability to Industry Members would also weaken the overall cyber program of CAT.[114] The Participants expressed concern that CAT LLC is not equipped to compensate Industry Members in the event of a data breach because funding is designed to cover costs only.[115] The Participants further assert that it is difficult to imagine how CAT LLC could ensure solvency if substantial exclusions are included in a limitation of liability.[116] However, these are not compelling reasons to include the proposed Limitation of Liability Provisions. The Commission believes that there are mechanisms in place to ensure CAT LLC will not fail to compensate Industry Members or become insolvent. Specifically, the Participants are obligated to maintain a CAT and cannot dissolve CAT LLC without Commission approval.[117] Due to its obligation to maintain the CAT, the Participants would need to fund CAT LLC by recovering any shortfall from the Participants and/or Industry Members.[118] To the extent the Participants seek to recover any shortfall from Industry Members, the Commission will assess those fees to assure that they are reasonable.[119]

---

114 The CRA Response emphasizes that Industry Members and other interested parties are able to monitor and suggest improvements for CAT's cyber security and "history is replete with examples." See CRA Response at 3-4.

115 See Second Response Letter at 15.

116 See Second Response Letter at 15. See also CRA Response at 9 (stating that CAT LLC's "cost-only business model" provides no mechanism to establish safety reserves that might allow it to build a cash reserve to pre-fund catastrophic losses from a cyber breach).

117 See CAT NMS Plan, Article X, Section 10.1.

118 See CAT NMS Plan, Article XI, Section 11.1(b) and 11.2. Specifically, Section 11.1(b) states that subject to Section 11.2, the Operating Committee shall have discretion to establish funding for the CAT LLC, including: (i) establishing fees that the Participants shall pay; and (ii) establishing fees for Industry Members that shall be implemented by Participants. Section 11.2 sets forth funding principles that the Operating Committee should consider in establishing the funding of the Company. Specifically, Section 11.2(f) states that the Operating Committee should consider building financial stability to support the Company as a going concern.

119 See CAT NMS Plan, Article X, Section 11.1(b).

Even in the absence of the proposed Limitation of Liability Provisions, the Participants may have limited liability to Industry Members through court-established regulatory immunity.[120] To the extent it is available, regulatory immunity may create the same incentive as the proposed Limitation of Liability Provisions for Participants to reduce their investment in CAT cybersecurity. Regulatory immunity, however, is not applicable in all scenarios (i.e., commercial use or intentional misconduct). The Commission does not believe that the Participants have adequately explained why, in cases where regulatory immunity may not be applicable because Participant use of CAT data is improper (e.g., commercial use or intentional misconduct), they should be permitted to limit their liability. The potential consequences of such behavior, however, could also fall on Industry Members who have no control over the security of CAT Data they have submitted to the CAT. The Commission believes that the presence of liability risk would provide Participants an additional incentive to invest in CAT data security to prevent such behavior from occurring.[121] The Commission believes that the Participants have not met their burden to demonstrate that the Proposed Amendment is necessary or appropriate in the public interest, for the protection of investors and the maintenance of fair and orderly markets, to remove impediments to, and perfect the mechanisms of, a national market system, or otherwise in furtherance of the purposes of the Exchange Act.[122]

C. Breadth of the Proposed Limitation of Liability Provisions

Several commenters are critical of the scope of the proposed Limitation of Liability Provisions and in particular the language that prohibits Industry Members from pursuing claims against CAT LLC and the Participants if there is "willful misconduct, gross negligence, bad faith

---

120 See Section IV.C.1, supra. The Participants assert that regulatory immunity applies to their use of CAT. See Response Letter at 23; Second Response Letter at 4.

121 See also Economic Analysis at Section V.A.

122 17 CFR 201.700(b)(3).

or criminal acts of CAT LLC, the SROs or their representatives or employees."[123] As one commenter states, the proposal would shield the Participants from liability, "not only for a breach of the CAT System by malicious third-party actors but even from the theft or other misuse of CAT Data by SRO employees" and would "effectively extinguish the liability of CAT LLC and the SROs even in instances of gross negligence or intentional misconduct."[124] Another commenter states that the proposal "would effectively hold brokers responsible for the malfeasance and incompetence of the SROs and their contractors" and that this would be "extremely unreasonable."[125]

A commenter suggests that if the limitation of liability language was adopted as proposed, "CAT LLC would only have $500 in liability if an SRO employee stole CAT Data and posted it on the internet."[126] A commenter believes that liability cap should only apply when CAT LLC and the Participants are acting solely in their regulatory capacity, for which they have proposed a definition, and should exclude willful misconduct, gross negligence, bad faith, or criminal acts.[127]

The Participants state that the proposed Limitation of Liability Provisions fall squarely within industry norms, referencing a comparison to the allocation of liability between Industry Members and SROs in other regulatory contexts, including NMS plans, regulatory reporting facilities, SRO rules and liability provisions that Industry Members use to protect themselves when they possess sensitive customer and transaction data.[128] The Participants believe that the

---

123 See SIFMA Letter at 5, 7-8. See also LPL Financial at 1; FIA PTG Letter at 2; Raymond James Letter at 2; Citadel Letter, at 3 (stating that the provisions would protect Participants and their representatives from any and all potential misuse, including intentional misuse, of CAT Data); SIFMA Letter II at 8-9.

124 See SIFMA Letter at 5; see also LPL Financial at 1; FIA PTG Letter at 2; Raymond James Letter at 2.

125 See ASA Letter at 2.

126 See SIFMA Letter II at 8.

127 See SIFMA Letter II at 11.

128 See Response Letter at 5-11.

proposed Limitation of Liability Provisions are "substantively identical" to the liability provisions to which Industry Members regularly agree in connection with OATS reporting.[129]

Commenters, however, dismiss comparisons made in the Proposed Amendment to OATS limitation of liability provisions because (1) CAT captures significantly more information than OATS, including personally identifiable information, and data reported to OATS is reported to and only used by FINRA; and (2) OATS does not have account-level data, which the CAT will collect and which could present the risk of reverse engineering of trading strategies.[130] One commenter stated that the limitation of liability provisions for OATS were signed in 1998, and since then the landscape of cybersecurity has changed, and the frequency and scale of data breaches has increased dramatically.[131]

In response, the Participants reject the suggestion that any limitation of liability provision should allow liability for willful misconduct, gross negligence, bad faith or criminal acts of CAT LLC, the SROs or their representatives or employees.[132] The Participants assert that the exclusion of "gross negligence, willful misconduct, bad faith, or criminal acts" is not appropriate and would be inconsistent with other limitation of liability provisions for other NMS plans (including OATS) and SRO rules.[133] The Participants state that in the limited instances in which

---

129 Id. at 6-7. Commenters assert that the proposed Limitation of Liability Provisions are inconsistent with industry standards, citing among other things SRO limitation of liability rules which exclude protection for willful misconduct, gross negligence, bad faith or criminal acts. See SIFMA Letter at 7; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2; Fidelity Letter at 2.

130 See Lewis Paper at 9-10; SIFMA Letter at 8; LPL Financial Letter at 2; Raymond James Letter at 2; FIA PTG Letter at 2; Virtu Letter at 4; SIFMA Letter II at 7.

131 See Lewis Paper at 10.

132 See Response Letter at 7 (citing SIFMA Letter at 7-8); Second Response Letter at 4; 13-15.

133 See Second Response Letter at 4, 13-15. The Participants assert that the proposed Limitation of Liability Provisions are consistent with SRO limitation of liability rules, emphasizing that under those rules the SROs generally have the discretion, but not obligation, to compensate harmed Industry Members, and that this discretion only applies in very limited circumstances—namely, for system failures that impact the execution of individual order. See Response Letter at 5-6. The Participants also note that during

SRO liability rules permit claims for gross negligence or willful misconduct, Industry Members are often prohibited from suing an SRO for damages unless the alleged gross negligence or willful misconduct also constituted a securities law violation for which Congress has authorized a private right of action.[134] The Participants further argue that modifying the proposed Limitation of Liability Provisions is not supported by the CRA Paper, because such modifications would likely result in litigation over liability[135] and litigation to prove these elements even if non-existent.[136]

The CRA Response also states that the comment letters do not acknowledge that behavior falling in these categories is already subject to enforcement by the Commission.[137] The Participants state that the Commission's regulatory enforcement regime and the potential for severe reputational harm already sufficiently incentivize the Participants not to engage in bad

---

negotiations, the Participants submitted to SIFMA a term sheet that provided for a discretionary compensation mechanism modeled after SRO rules, which was rejected by SIFMA. See Response Letter at 6. See also Second Response Letter at 13-14. The Participants state that no SRO limitation of liability rule contemplates SRO liability for "catastrophic" damages resulting from the theft of Industry Members' proprietary trading algorithms. See Response Letter at 6.

134 See Response Letter at 6-7. Thus, the Participants believe that that these provisions would not provide for liability against the self-regulatory organizations in the event of a data breach. Id. at 7-8. See also Second Response Letter at 13-14 (stating that SRO rules that contain exclusions generally are modified by other rules that broadly prohibit Industry Members from suing the exchanges or their representatives, except for violations of the federal securities laws for which a private right of action exists, and thus the Participants do not believe these provisions would provide for liability against the SROs in the event of a data breach).

135 See, e.g., Response Letter at 9; CRA Response at 18.

136 See Response Letter at 9; Second Response Letter at 4, 14-15. According to the Participants, although they, CAT LLC, and FINRA CAT may ultimately be found not liable, such litigation would be expensive, time-consuming, would distract Participants from their regulatory oversight mandate, and may open the doors of discovery to potentially malicious actors. See Response Letter at 9.

137 See CRA Response at 18. The CRA Response also argues that including commenters' proposed exclusions to the Proposed Limitation on Liability Provisions would potentially generate substantial litigation and that reducing expected liability costs may provide additional resources to enhance CAT's cyber security, purchase more cyber liability insurance (as it becomes available), or invest in competing CAT priorities. See CRA Response at 18-19.

faith, recklessness, gross negligence, and intentional misconduct, and so adding exclusions to the proposed Limitation of Liability Provisions would not result in any meaningful improvement to the CAT's cybersecurity.[138]

As noted in the previous section,[139] commenters believe that the CRA Paper only focuses on a breach by external actors and fails to address the risk of misuse of CAT Data by personnel at CAT LLC and the SROs.[140] The CRA Response argues that the CRA Paper did not specifically address the misuse of CAT Data by CAT personnel and other internal sources because whether a perpetrator is external or internal makes no difference to the scenario analysis.[141] The CRA Response also argues that the purported concerns about the threat of "internal" breaches are exaggerated and that all Participant users of CAT Data are subject to comparable cyber security procedures and protocols, and only trading data, not customer data, can be downloaded in bulk.[142]

---

138 See Response Letter at 9. The Participants note that enforcement actions could be brought for cybersecurity-related violations (e.g., failure to comply with Regulation SCI) and violations of the CAT NMS Plan (e.g., for violating the CAT NMS Plan by using CAT Data for non-regulatory purposes). See id. at 25-26. The Participants also state that the purpose of the CAT and the Participants' mandate under the CAT NMS Plan is the fulfillment of regulatory functions, and not operation in connection with business activities. Id. at 22. In addition, the CRA Response states that the comment letters do not acknowledge that behavior falling to these categories is already subject to enforcement by the Commission. See CRA Response at 18.

139 See infra Section IV.A.

140 See Citadel Letter at 6; SIFMA Letter at 9; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2; Virtu Letter at 5. One commenter states that the CRA Paper does not provide any support for the argument that broker-dealers should be accountable for the wrongdoing or misuse of data by SRO employees or contractors. See ASA Letter at 2.

141 See CRA Response at 19. As noted earlier, Participants also state that the CRA Paper did not make any assumptions regarding the identity of potential bad actors or where they may work, and the CRA Paper was not intended to predict every possible scenario, but instead intended to provide an illustrative framework to assess the economic exposures that flow from the gathering, storage, and use of CAT Data. See Response Letter at 15-16 (citing CRA Paper 2).

142 See CRA Response at 20.

The Commission does not believe that the Participants have demonstrated that it is necessary or appropriate to foreclose all potential Industry Member claims, including those arising from "gross negligence, willful misconduct, bad faith, or criminal acts" to a maximum of $500 per Industry Member per calendar year as proposed.[143] The Commission believes that the damages to Industry Members for breaches of CAT could potentially far exceed that amount, and Participants and the CRA Response acknowledge the possibility for low frequency events with extreme severity.[144] For example, as discussed above, the CRA Paper estimates an exposure of at least $100 million per incident would be reasonable if an algorithmic trading firm's strategy was reverse engineered, and if the Proposed Amendment were adopted the Participants would only have $500 in liability to the trading firm even if the trading strategy was exposed through gross negligence, willful misconduct, bad faith, or criminal acts. This means that the proposed Limitation of Liability Provisions would shield the Participants from liability to Industry Members even if a Participant intentionally used CAT Data for competitive business purposes, or an employee of CAT LLC sold CAT Data to a foreign government.

As noted above, Participants can assert regulatory immunity to the extent that the doctrine applies if there is a security breach that exposes CAT Data and Industry Members seek damages from the responsible Participants.[145] However, the Commission believes that for situations where regulatory immunity may not be applicable (e.g., commercial use or intentional misconduct), the Participants have not met their burden to justify a nearly complete elimination of liability to Industry Members as consistent with the Exchange Act and the rules and

---

143 As discussed above, a number of factors impact the Participants' incentives to invest in, or prioritize, the security of the CAT. See Section IV.B., supra. The Commission does not believe that the Participants have met their burden of establishing that it is appropriate to foreclose liability to Industry Members for potential claims arising from "gross negligence, willful misconduct, bad faith, or criminal acts" because of the Commission's regulatory enforcement regime and the potential for severe reputational harm.

144 See notes 104 and 105, supra, and accompanying text.

145 See Section IV.B, supra.

regulations as required by Rule 608 of Regulation NMS, as discussed above. The Commission cannot make a finding that the proposed amendment is consistent with the Exchange Act and the rules and regulations issued thereunder.[146]

V. Impact on Efficiency, Competition, and Capital Formation

In determining whether to approve a CAT NMS Plan amendment, and whether such amendment is in the public interest, Rule 613 requires the Commission to consider the potential effects of the proposed amendment on efficiency, competition and capital formation.[147] The Commission has reviewed the arguments about such effects put forth by the Participants and commenters and independently analyzed the likely effects of the Proposed Amendment on efficiency, competition and capital formation.. Many of those effects hinge on assumptions about the applicability of the doctrine of regulatory immunity in the case of litigation related to a breach of CAT Data, the influence of such immunity on the incentives of the Participants to protect the CAT Data, and the potential redundancy of a limitation on liability if immunity applies. Commenters have addressed the applicability of this doctrine directly in their comments,[148] many of which relate to two studies: the CRA Paper submitted by the Participants as part of their filing, and the Lewis Paper submitted by SIFMA as part of its commentary;[149] both of these studies make assumptions regarding regulatory immunity that impact their respective conclusions. In the case of the CRA Paper, many conclusions stem from an assumption that regulatory immunity would not apply and thus Participants would be faced with significant risk of litigation in the case of a CAT data breach that resulted from the collection of CAT Data into the central repository or the use of that CAT Data by a Participant that was performing its regulatory duties. In the case of the Lewis Paper, many of the conclusions are

---

146 17 CFR 201.700(b)(3); 17 CFR 242.608(b)(2).

147 17 CFR 242.613(a)(5).

148 See, e.g., Citadel Letter at 1, 3-5; SIFMA Letter at 8; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2.

149 See Lewis Paper, supra, note 27.

based on an assumption that, if the Proposed Amendment were allowed, Industry Members, as opposed to Participants, would bear significant liability in the case of a data breach because the limitation of liability would be absolute, the Lewis Paper does not address the doctrine of regulatory immunity[150] as it might apply to Participants.[151]

In summary, the Commission believes that, if approved, the Proposed Amendment would likely have significant negative effects on efficiency, though minor positive effects that are unlikely to significantly mitigate the negative effects are also discussed below.[152] The Commission believes the Participants are best poised due to information asymmetry to understand the risks inherent in collecting and using CAT Data, and, because of moral hazard, to mitigate those risks through operational measures to promote CAT data security and securing insurance to mitigate financial risks associated with CAT data security. Efficiency is likely to be reduced to the extent the Proposed Amendment disincentivizes the Participants from investing in CAT data security and thus potentially increases the likelihood of a data breach. The Commission believes this effect would be only partially mitigated as discussed below and believes the net effect may remain significant. The Commission believes that the Proposed Amendment might have negative effects on competition and capital formation, but believes these effects would be partially mitigated. These conclusions are discussed in the analysis which follows.

A. Efficiency

---

150 The Commission recognizes that the Participants believe regulatory immunity would apply in the event of a breach concerning CAT Data (*see* Response Letter at 23; Second Response Letter at 4), but the Participants also believe that there is no guarantee that all courts will agree that the Participants' immunity extends to the claims at issue. The Commission acknowledges that beliefs about regulatory immunity may influence the outcomes it describes in this analysis.

151 See, e.g., Lewis Paper at 4.

152 See Section V.A., infra.

The Commission believes that the Proposed Amendment would likely have a significant effect on efficiency, although minor positive effects that are unlikely to significantly mitigate the negative effects are also discussed below. These mixed effects would likely be dominated by the negative effects of reducing the Participants' incentives to invest in CAT data security. Generally, the Commission believes that the Proposed Amendment would reduce the Participants' incentives to invest in CAT data security. The Commission believes that taking measures that may prevent a data breach is inherently more efficient than remediating the consequences of a data breach after it has occurred.[153] Consequently, liability rules that incentivize appropriate security measures are likely to increase efficiency while rules that potentially disincentivize Participants from securing CAT Data may reduce efficiency. As noted, the magnitude of this effect hinges on the Participants' beliefs about the applicability of the doctrine of regulatory immunity. If the Participants do not believe regulatory immunity applies to all aspects of their collection and use of CAT Data, or have significant uncertainty that it would apply to some or all aspects, the Proposed Amendment would represent to the Participants a shift of liability from the Participants to Industry Members, the magnitude of which would be a function of the level of Participant uncertainty about their regulatory immunity.[154] Absent the Proposed Amendment, the Participants might make further investments in data security beyond those mandated by the CAT NMS Plan and Commission rulemakings such as implementing internal controls designed to decrease the likelihood of misuse of CAT Data. But the assurance of limited liability provided by the Proposed Amendment could disincentivize such actions or even incentivize a reduction in existing investments in cybersecurity.

---

153 See, e.g., Securities Exchange Act Release No. 89632 (Aug. 21, 2020), 85 FR 65990, 66091 (Oct. 16, 2020) (proposing amendments to the CAT Plan to enhance data security).

154 The proposed Limitation of Liability Provisions would limit liability to $500 per CAT Reporter or CAT Reporting Agent in a calendar year. See Notice, supra note 5, 86 FR at 593. See Section V.A, infra, for discussion of liability for Industry Members that do not carry customer accounts.

The CRA Paper maintains that additional investment in security such as providing additional insurance, may not be efficient. The CRA Paper states, "…the prospect of litigation arising from the absence of the limitation on liability provision has the prospect for prompting overpayment for cyber security on the part of the CAT and the Plan Processor beyond the economically optimal level of protection, despite the analysis we present above suggesting that such litigation would provide no incremental benefit. The prospect of third-party litigation may prompt CAT LLC to expend resources on cyber security systems that supplement the detailed (and regularly updated) framework implemented by the Commission, but that do not reduce the cyber risk commensurate with the costs."[155] The CRA Paper further argues that the threat of third-party litigation may result in risk-aversion that prevents the Participants from adopting policies or technologies that decrease costs or increase efficiencies.[156] The Commission agrees with the CRA Paper that there are likely to exist certain security investments that do not provide sufficient benefits to warrant their adoption, particularly in light of the Commission's belief that investors may ultimately bear the costs of these investments—as well as costs of potential litigation.[157] However, the Commission disagrees that litigation risk provides no incremental benefit because the threat of such litigation may incentivize the Participants to implement security measures such as the adoption of internal controls that decrease the likelihood of an employee or contractor making commercial or other misuse of CAT Data.[158] Further, the Commission recognizes that while the Participants face costs in the event of a CAT data breach, these costs are likely to fall upon broker-dealers and investors as well, while these groups have limited ability to participate in decisions related to investments in CAT security. This

---

155 The CRA Paper discusses reasons why the incremental benefit from litigation from Industry Members may be reduced, but does not show that there is no incremental benefit. See Notice, supra note 5, at 616-17.

156 See Notice, supra note 5, at 617-18.

157 The Commission has the power to disallow fee amendments that might unfairly pass costs to Industry Members.

158 See note 113, supra, and referring text.

partitioning of decision-making authority from the financial consequences of the decision creates an agency problem that may limit the Participants' incentives to select the welfare-maximizing level of security investment. This agency problem may be partially mitigated by the Participants' perception of litigation risk in the event of a data breach by better aligning their incentives regarding security decisions with other parties that are likely to be harmed if such a breach occurs.

The Commission recognizes that the risk of the Proposed Amendment disincentivizing the Participants from taking additional measures to ensure security is likely to be partially mitigated by other incentives that are not impacted by the limitation on liability. Independent of potential regulatory immunity,[159] Participants face significant costs, both direct and indirect, that would result from a data breach. The potential reputational consequences of a data breach would likely be severe and such a breach is likely to draw significant negative publicity, public scrutiny, and attention from regulatory and other government entities. Further, while contractual limitation of liability reduces the risk of exposure, it does not prevent enforcement actions from the Commission or litigation by parties other than Industry Members. In addition, any breach would likely cause a significant disruption to Participants' own operations[160] and some breach threats are not about compromising data but are indeed designed to disrupt operations;[161] Participants are thus still incentivized to create security measures that mitigate the risk of such breaches, which likely help mitigate the risk of compromised data that could directly affect

---

159 The Commission believes the Participants' views on their potential regulatory immunity with regard to CAT data collection and use is immaterial to this second set of incentives because these consequences of a data breach could occur regardless of whether there could or would be litigation as a result of that breach.

160 A breach of CAT data could occur in a Participant's own analytic or operational environment.

161 See, e.g., Raphael Satter, Up to 1,500 businesses affected by ransomware attach, U.S. firm's CEO says, Reuters (July 6, 2021), available at https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/.

Industry Members. However, the Commission believes that decreasing the risk of exposure that Participants face through the Proposed Amendment will likely on balance disincentivize the Participants from investing in data security, particularly if the proposed amendments increase the scope of immunity that might be expected beyond regulatory immunity.[162]

The Commission believes that taking measures that may prevent a data breach is more efficient than remediating the consequences of a data breach after it has occurred.[163] Consequently, measures that incentivize appropriate security measures are likely to increase efficiency while measures that potentially disincentivize Participants from securing CAT Data may reduce efficiency.

As noted above, several commenters express concern that shifting liability through the proposed Limitation of Liability Provisions would reduce the incentives of Participants to develop robust data security and risk mitigation mechanisms, and may even incentivize the Participants to de-prioritize data security.[164] The Commission believes, however, that the degree to which the proposed amendment would disincentivize the Participants from appropriate security measures is dependent upon the Participants' belief in the applicability of regulatory immunity to the collection and permitted uses of CAT Data in the absence of the proposed amendment. The Commission believes that uncertainty regarding liability in case of a CAT data breach thus serves as an incentive for the Participants to invest in data security to the extent that Participants believe a court might not uphold their regulatory immunity or it would be judged not to apply in a given case that was before the courts. If the Participants believe that regulatory

---

162 See Sections V.B and V.C, supra.

163 See, e.g., Securities Exchange Act Release No. 89632 (Aug. 21, 2020), 85 FR 65990, 66091 (Oct. 16, 2020) (proposing amendments to the CAT Plan to enhance data security).

164 See, e.g., Lewis Paper at 5-9, 14; SIFMA Letter at 7, 9; LPL Financial Letter at 1; Raymond James Letter at 2; FIA PTG Letter at 2; Virtu Letter at 3; ASA Letter at 2; Fidelity Letter at 2; Citi Letter at 2.

immunity is likely to apply, the proposed amendments would serve to reduce their risk of incurring costs of litigation by reducing the likelihood of litigation by Industry Members.

Some commenters addressed the scope of the limitation of liability, considering whether Participants might be shielded from liability in commercial use of CAT Data,[165] even though such use is prohibited by the CAT NMS Plan.[166] Another commenter focused on the scope of the immunity more generally as it would appear to exceed the bounds of conventional regulatory immunity.[167] One commenter characterized the economic structure as creating a "moral hazard" and stated that permitting litigation against Participants and their representatives when they are acting outside their regulatory capacity is "crucial" and would give the Participants very strong financial incentives to invest heavily to prevent or minimize the likelihood of such failures.[168]

To the extent that the scope of limitation of liability in the Proposed Amendment exceeds what might be expected from the doctrine of regulatory immunity, an expansion of the scope of activities that could be shielded from liability would potentially further disincentivize Participants from activities that promote CAT data security even if regulatory immunity applies.

The Commission also recognizes that the Proposed Amendment may reduce the risk of litigation in the event of a breach by resolving the existing uncertainty about whether the Participants could be liable; in other words, if Industry Members know they cannot recover due to the limitation of liability, regardless of the applicability of regulatory immunity, they may be less likely to sue over a breach. Such litigation would impose costs, both direct and indirect,[169] on the Participants to defend themselves even if they would ultimately prevail due to regulatory

---

165 See, e.g., SIFMA Letter at 8; LPL Financial Letter at 1; FIA PTG Letter at 2; Raymond James Letter at 2.

166 See, e.g., CAT NMS Plan Sections 6.5(f)(i)(A); 6.5(g).

167 See Citadel Letter at 5.

168 See Citi Letter at 2. In response, the CRA Response argues that the structure might not be considered a classic "moral hazard" due to Industry Members' ability to monitor and influence CAT cyber security. See CRA Response at 10-11.

169 Indirect costs would include opportunity costs of time and effort spent dealing with litigation. See, e.g., Notice, supra note 5, 85 FR at 617-618; Response Letter at 8-9.

immunity and those direct costs might be passed on to Industry Members and ultimately investors. The Proposed Amendment would reduce the likelihood of litigation and thus might avoid costs associated with litigation that investors would unnecessarily bear, which could improve efficiency. Additional insurance costs to Industry Members related to liability risks from the Proposed Amendment are discussed below.

While both the CRA Paper and the Lewis Paper frame their analyses from a perspective of potential litigation, the Commission notes that not all potential data breaches are amenable to litigation. The Commission believes that a data breach could go undetected, particularly if such a breach were perpetrated by authorized users of the CAT System such that detection of the breach relied primarily on the Participants' screening of their employees and contractors before providing access to CAT Data and then the monitoring of their use of CAT Data when they became authorized users.[170] Such a breach could impose significant costs on Industry Members if their intellectual property (such as proprietary trading strategies) were revealed to competitors or bad actors. Consequently, the Commission believes that reducing the Participants' existing incentives to properly invest in data security activities might disincentivize individual Participants from appropriately investing in the screening and monitoring of their own employees and contractors that will access CAT Data. This might reduce efficiency by increasing the likelihood of a breach either detected or undetected.

In addition, the Proposed Amendment might improve efficiency by promoting the optimal level of usage of CAT Data.[171] Specifically, if the Participants believe their regulatory immunity may not be recognized in litigation in the wake of a data breach, they may be

---

170 Several commenters discussed arguments in the CRA Paper and Lewis Paper regarding ex-ante regulation versus ex-post litigation. See Citadel Letter at 1-2, 7; Lewis Paper at 7-9. An undetected breach cannot be addressed through litigation, but might be prevented by ex-ante regulation or the proper alignment of incentives in lieu of regulation. The Commission considers screening of potential users of CAT Data and monitoring their activities with CAT Data to be security activities that would be affected by Participant incentives to prevent data breaches.

171 See CAT NMS Plan Approval Order, supra note 1, at 84833-40.

incentivized to minimize their use of CAT Data to minimize opportunities for a data breach, particularly one involving their own employees or contractors. However, the Proposed Amendment might facilitate increased use levels of CAT Data by Participants by reducing the risk of exposure to litigation. Consequently, the Commission believes that the Proposed Amendment might prevent inefficiencies related to underuse of CAT Data by regulators. By contrast, to the degree that disapproval of the Proposed Amendment renders regulators more risk averse in using CAT Data to meet their regulatory obligations than they would be if the Proposed Amendment were approved, disapproval may reduce use of CAT Data by regulators. Further effects on efficiency depend upon the use of insurance by Participants and Industry Members. The Lewis Paper and the CRA Paper analyze the potential for the use of insurance by Participants and Industry Members to manage the financial risks of a potential data breach.[172] Through the CRA Paper, the Participants argue that adopting the Proposed Amendment would avoid inefficiencies such as over investment in insurance beyond what would be optimal.[173] The CRA Paper argues that this inefficiency would result in unnecessary costs being passed to investors without a corresponding societal benefit.[174] The Lewis Paper argues that shifting the financial risks of a CAT data breach to Industry Members by limiting liability for Participants would cause them to insure against the financial consequences of a CAT data breach, which would be inefficient because Industry Members cannot give an insurer access to the CAT System to monitor or assess the security of the system. Consequently, according to the Lewis Paper, insurance purchased by Industry Members to cover the risk would be more expensive, and investors would ultimately bear this increased expense.[175] Also, policies obtained by Industry Members would necessarily overlap, further increasing the cost of such insurance.[176] Other

---

172 See Lewis Paper at 11-14; Notice, supra note 5, at 618-620.

173 See Notice, supra note 5, at 617-18.

174 See Notice, supra note 5, at 617-18.

175 See Lewis Paper at 11-14.

176 See Lewis Paper at 14.

commenters supported the position that the Participants can more efficiently obtain cyber insurance.[177]

The Commission agrees that the Participants are better positioned to insure against a breach both due to their ability to provide access and monitoring of the CAT System to an insurer, and because if Industry Members were to obtain insurance that would apply to a CAT data breach, such policies would overlap because the same breach event would likely impact multiple Industry Members and many investors whose data might be exposed in a breach are customers of multiple Industry Members. However, as noted by some commenters, the doctrine of regulatory immunity may already shift significant breach risk to Industry Members,[178] and the Participants state that Industry Members may already shift some of their own risk of data breaches to their own customers with their own limitation of liability language in customer agreements.[179] Further, as discussed above, insurance is unlikely to provide a remedy in case of breaches that go undetected. However, the Commission recognizes that if the doctrine of regulatory immunity does not apply, the Proposed Amendment would shift the financial risks of a breach to Industry Members. The Commission believes that investors are likely to bear the costs of providing security to the CAT System as well as any costs of a breach of CAT Data. However, the Commission recognizes that inefficiencies in providing security to CAT are likely to increase the costs that investors bear.

The Commission believes that, even if the Proposed Amendment were approved, inefficiencies in the scope and maintenance of Industry Member insurance policies against a CAT data breach are likely to be minor for two reasons. First, Industry Members that carry customer accounts already face risks related to breach of customer information. The

---

177 See SIFMA Letter at 8-9; LPL Financial Letter at 2; FIA PTG Letter at 2; Raymond James Letter at 2; Virtu Letter at 3-4.

178 See Section IV.C.1, supra.

179 See Response Letter at 10.

Commission believes these Industry Members actively manage the security of their environments to prevent a breach of this data within their systems and acknowledges that they cannot continue to safeguard this data once this it data is reported to CAT. However, as noted by commenters, Industry Members also typically indemnify themselves with agreements that limit their liability in the case of a data breach and thus would be unlikely to increase their insurance coverage if the proposed amendments were approved. Second, any additional insurance burdens would likely to be negligible for Industry Members that carry no customer accounts because they do not risk litigation from customers. However to the degree that Industry Members overall would increase cyber insurance to offset this risk if the Proposed Amendment is approved, the cost of such insurance would likely to be higher than it would be if the risk were borne by Participants because Industry Members cannot facilitate the monitoring of an insurer and the policies Industry Members would purchase would necessarily be overlapping policies because investors often have accounts with multiple Industry Members and a single data breach might expose data from multiple Industry Members. Those inflated costs would ultimately be passed to investors, and the security improvements that might be facilitated by the monitoring of an insurer contracted by the Participants would be unrealized.

B. Competition

The Commission believes that the Proposed Amendment might have negative effects upon competition, but believes these effects would be partially mitigated. In their filing, the Participants state they do not believe the Proposed Amendment will have any impact on competition.[180] However, the Commission believes that the Proposed Amendment could have negative effects on the competitive positions of some Industry Members relative to other Industry Members. Industry Members have diverse business models; some of these models employ proprietary trading strategies that might be revealed in the wake of a data breach. If such

---

180 See Notice, supra note 5, at 597.

proprietary strategies were revealed, Industry Members that employed such strategies might experience loss of intellectual property that could damage their competitive positions relative to their peers. The Commission further acknowledges that a data breach could harm an Industry Member's reputation and damage its competitive position within the markets in which it competes, particularly if customer data were released from some but not all competitors within those markets. The Commission acknowledges that robust investment in cyber security does not guarantee breaches will not occur. The likelihood of a data breach happening however, increases if Participants reduce potential additional investment in CAT data security including additional investment in cyber insurance coverage (should such coverage become available) or additional investment in the screening and monitoring of employees and contractors that have access to CAT Data. But the assurance of limited liability provided by the Proposed Amendment could disincentivize such actions. The Commission believes that Participants would remain incentivized to invest in CAT data security to some extent, even if the Proposed Amendment is approved because of the additional incentives discussed above, such as reputational damage, which would remain unaffected by the Proposed Amendment.[181]

The Commission further believes there might be additional competitive effects of the Proposed Amendment in the market for trading services. The Commission recognizes that Industry Members are not just the customers and members of the Participants, but are sometimes competitors of the Participants. Exchanges (all of which are Participants) compete in the market for trading services with off-exchange venues such as alternative trading systems (all of which are operated by Industry Members) and Industry Members that provide liquidity to orders off-exchange.[182] Consequently, if the Proposed Amendment were to shift any of the expense of insuring against the risk of a CAT data breach from Participants to Industry Members, and if such expenses were more efficiently borne by Participants as discussed previously, the additional

---

181 See Section VI.A., supra.

182 See CAT Plan Approval Order, supra note 1, at 84882-89.

marginal costs incurred by Industry Members could disadvantage them in this competition to provide trading services. However, the Commission believes that this effect would be partially mitigated because, as discussed previously, that even under the Proposed Amendment, the Participants would remain incentivized to invest in CAT data security, and that Industry Members' need to invest in additional insurance would be mitigated by their own use of limitation of liability agreements with their own customers.[183]

C. Capital Formation

The Commission believes that the Proposed Amendment might have negative effects on capital formation in markets in which Industry Members compete, but believes these effects would be partially mitigated.

The Participants argue that adopting the proposed amendment would avoid inefficiencies by avoiding the increased costs that would otherwise arise,[184] namely over investment in cyber security and insurance beyond what would be optimal, and underinvestment in adoption of policies or technologies that decrease costs or increase efficiencies as described in the CRA Paper. The Participants argue that avoiding these issues, by limiting liability, would promote capital formation in the U.S. securities markets. While the Commission acknowledges that an inappropriate level of risk-aversion might result in these effects, if the Participants believe, as asserted in their filing, that they have regulatory immunity, the Commission believes these effects would be small because the potential shift in liability from the proposed amendments would be far less significant than anticipated in the CRA Paper.

It is possible that capital formation could be negatively impacted by an inefficient insurance burden on Industry Members as described in the Lewis Paper.[185] However, even in cases in which Participants' regulatory immunity would not apply, the Commission does not

---

183 See Section VI.A., supra.

184 See Notice, supra note 5, at 617-18.

185 See Lewis Paper at 11-14.

believe the Proposed Amendment would significantly increase Industry Members' insurance burden because, as discussed previously, many Industry Members have agreements limiting their liability with their own customers, and not all Industry Members have customers that might initiate litigation.[186]

The Commission recognizes, however, that the risk of a data breach can impact capital formation through routes other than inefficient insurance costs and underinvestment. If Industry Members believe that the proposed amendment would significantly reduce Participants' incentives to invest in CAT security, Industry Members may be less incentivized to invest in intellectual property that could be compromised by a data breach, potentially reducing capital formation in liquidity provision on exchanges or in proprietary trading activities. The Commission believes this risk is partially mitigated because the Participants are still incentivized to secure CAT Data by other incentives that are not affected by the proposed amendment.[187]

---

186 See Section VI.A, supra.

187 See Section VI.A, supra.

VI. Conclusion

For the reasons set forth above, the Commission does not find, pursuant to Section 11A of the Exchange Act, and Rule 608(b)(2) thereunder, that the Proposed Amendment is consistent with the requirements of the Exchange Act and the rules and regulations thereunder applicable to an NMS plan amendment.

IT IS THEREFORE ORDERED, pursuant to Section 11A of the Exchange Act, and Rule 608(b)(2) thereunder, that the Proposed Amendment (File No. 4-698) be, and hereby is, disapproved.

By the Commission.

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2021-24035 Filed: 11/3/2021 8:45 am; Publication Date: 11/4/2021]